DENISE M. MINGRONE (SBN 135224)
dmingrone@orrick.com
ROBERT L. URIARTE (SBN 258274)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
Telephone: +1 650 614 7400
Facsimile: +1 650 614 7401

Attorneys for Plaintiff/Counterdefendant
SYNOPSYS, INC.

JENNIFER LEE TAYLOR (SBN 61368)
JTaylor@mofo.com
STACEY M. SPRENKEL (SBN 241689)
SSprenkel@mofo.com
JOYCE LIOU (SBN 277720)
JLiou@mofo.com
AMANDA D. PHILLIPS (SNB 305614)
APhillips@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105
Telephone: +1 415 268-7000
Facsimile: +1 415 268-7522

Attorneys for Defendants
UBIQUITI NETWORKS, INC.,
UBIQUITI NETWORKS
INTERNATIONAL LIMITED and
CHING-HAN TSAI

December 15, 2017

Hon. William Orrick III
United States District Court
450 Golden Gate Ave., Box 36060
San Francisco, CA 94102

Re: *Synopsys Inc. v. Ubiquiti Networks, Inc. et al.*: 3:17-cv-561: Discovery Dispute re Requests for Forensic Inspection and Imaging

Dear Judge Orrick:

Pursuant to Rule 4 of Your Honor's Standing Order for Civil Cases, the parties submit this joint statement to seek resolution of a discovery dispute. Counsel for the parties have met in person twice in an attempt to resolve these issues, without success.

I. SYNOPSYS' POSITION

Synopsys' claims arise from Defendants' trafficking and use of counterfeit license keys to pirate Synopsys' software. Synopsys' software transmits basic system information about computers using counterfeit license keys, including a computer's MAC address, IP address, and server host name ("call-home data"). Call-home data for Defendants' piracy identifies computers bearing 14 MAC addresses associated with 15 distinct user names. These are the computers Synopsys seeks to inspect.

Synopsys served its request to forensically inspect the subject computers on September 8, 2017. Defendants wholesale refused to produce any devices on October 9. *See* Exhibits 1-4. After several laborious meet and confer sessions and weeks-long efforts to compose a joint submission, on November 29, Defendants asserted for the first time several new arguments, including a new argument that the forensic inspection requested herein should be delayed pending Defendants' summary judgment motion on Synopsys' DMCA claims. Defendants also argue that they will produce unspecified "logs" that obviate the need for inspection, but offer no detail as to what the logs contain. Defendants' positions all lack merit, and their dilatory conduct should not be countenanced.

Extraterritoriality. Synopsys does not agree that the DMCA has no extraterritorial application. But this issue is a complete red herring for purposes of discovery. Evidence of Defendants' off-shore activity will support (1) Defendants *domestic* DMCA claims, including on the issues of counterfeit key trafficking and willfulness; and (2) Synopsys' claims for fraud, label trafficking, and RICO predicate acts that aren't subject to Defendants' DMCA extraterritoriality argument. For example, inspection of Defendants servers will provide evidence of network topography, configuration files, and virtual machine artifacts that cannot possibly be reflected in Defendants mystery "logs." This evidence will shed light on how Defendants remotely accessed, *from computers in the U.S.*, Synopsys' software and license keys residing on those servers.

Good Cause. Defendants are network technology specialists who set up a sophisticated network of virtual machines, counterfeit key servers, and remote hosts that allowed Defendants to pirate Synopsys' software from dispersed geographic locations using anonymized IP addresses. Given the nature of this case and the piracy technology at issue, forensic inspection is appropriate. *See, e.g., Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 2009 U.S. Dist. LEXIS 40070, *2-5 (N.D. Cal. 2009) (granting inspection of servers that hosted infringing websites); *Ameriwood Indus., Inc. v. Liberman*, 2006 WL 3825291, at *4 (E.D. Mo. 2006) (noting proprietary of inspection where device itself is at issue). Defendants good cause arguments and citations below are all inapposite; they concern run-of-the-mill requests for emails and documents, whereas Synopsys seeks *forensic evidence* that can *only* be obtained through *forensic inspection*, such as forensic artifacts relevant to (i) use of key generators, (ii) use of piracy websites; (iii) external device usage; and (iv) user profiles. Moreover, Defendants' own discovery responses indicate that they have already deleted Synopsys' software and counterfeit keys from some subject computers. Similarly, Defendant Tsai apparently reconfigured Defendants' systems after Synopsys caught Ubiquiti red handed. Dkt. 85-1. Defendants' efforts to cover their tracks further support forensic inspection.

Relevance. Defendants contend that some of the requested computers do not contain relevant information because the users of the computers have professed their innocence. Synopsys need not blindly accept these representations in the face of contrary call-home evidence. *See Brocade Comms. Sys., Inc. v. A10 Networks, Inc.*, 10-CV-3428, 2012 WL 70428, at *1 (N.D. Cal. Jan. 9, 2012) (compelling forensic inspection). Moreover, Defendants' argument that Synopsys' call-home data might be inaccurate is not a basis to deny discovery. *See, e.g., Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 448 (D. Conn. 2010) (compelling imaging due to the strong "nexus between Genworth's claims and its need" for forensic evidence).

Burden. Defendants resist both inspection and copying based on two contradictory positions. Defendants contend that *inspection* of the subject devices would be unduly burdensome because installation of forensic tools risks causing "material alterations" to the inspected device. At the same time, Defendants resist *imaging* of the devices for inspection (which would eliminate the risk of any changes to the original device) because the devices purportedly contain trade secret and/or attorney-client privileged information, and because imaging of servers would take too long or would impair their availability. All of these arguments lack merit. First, with respect to non-server devices, Synopsys proposes to conduct a native inspection without installing any tools, followed by imaging so that tools can be used if necessary. With respect to Defendants' servers, Synopsys proposes a protocol in which Synopsys' experts would only natively inspect the servers without any imaging or installation of any forensic tools.[1] As to Defendants' trade secrets and privilege objections, Defendants can give the devices appropriate designations under the Protective Order. Notably, FTI's forensic inspection will not involve rummaging around through business documents or emails on the subject devices. FTI's inspection will be targeted at searching for specific forensic artifacts related to Synopsys' software and license key system.

Defendants' Pattern of Delay. Defendants initially argued that they could not produce the requested computers for inspection because they couldn't find them. During meet and confer sessions, Synopsys explained that its requests for inspection provided all the information Defendants needed to conduct a reasonable investigation and locate the subject computers, including IP addresses that point to the physical location of the computers, MAC addresses identifying the specific machines at issue, and computer "user names" that correspond to Defendants' employees (for example, the user name "jameslian" appears to correspond to a UNIL employee named James Lian). When the parties last met in person on November 8, we asked Defendants what computers they had located and counsel opaquely responded that their search for computers was "in process." But since the parties' November 8 meet and confer, Defendants have not indicated what additional devices they have located, choosing instead to invoke a series of new excuses and baseless arguments designed to further delay inspection.

For example, one of the key devices at issue in this motion is a 17-terabyte storage device that, *according to Defense counsel*, was the single device that remotely hosted Synopsys' software and license keys for remote use. Defendants argue disingenuously that the device "is so

[1] In lieu of installing tools, Synopsys' proposes a compromise whereby FTI will be given administrative access to Windows machines and root access to Linux machines to facilitate native inspection. This proposed compromise is made without prejudice to Synopsys' right to image servers if necessary.

complicated" that it cannot be *imaged*, but Synopsys has already agreed to inspect this device natively rather than image the device in the first instance. Synopsys even attempted to set up a conference call between the parties' respective forensics experts so that they could agree on an inspection protocol for the 17-terabyte device, but Defendants refused to cooperate. Defendants now complain that certain subject devices are "used daily in Defendants' largest R&D office for development and testing operations," and that discovery into the devices will impede such operations. Assuming that is true, Defendants have no cause to complain; they used these devices to pirate Synopsys' software and must deal with the consequences.

In sum, Defendants have already delayed providing any forensic discovery for months, and their new request to delay inspection for months more pending an unfiled summary judgment motion is neither justified nor feasible given the discovery schedule. Synopsys made great attempts to avoid the necessity of this motion, but with the close of fact discovery in February fast approaching, Synopsys was compelled to act. For the reasons stated, Synopsys respectfully requests that the Court order (1) native inspection and imaging of Ubiquiti and UNIL's responsive non-server devices,[2] and (2) native inspection of responsive servers, without prejudice to imaging of servers if necessary.

II. <u>DEFENDANTS' POSITION</u>

On September 8, 2017, Synopsys served 59 requests on each corporate defendant to inspect and copy a variety of "electronic devices" identified in the requests only by either (i) their use by specific individuals/usernames, (ii) MAC addresses, (iii) IP addresses, or (iv) host names. Synopsys claims that it based these forensic requests on "call-home data" it purportedly obtained from the Defendants' computers. During the parties' conferences, Defendants expressed concerns not only as to the sufficiency of the identifying information in Synopsys' requests, but also the accuracy of the underlying data, the burden it would impose on Defendants to produce all of the requested devices[3], and the proportionality of the requests without any information from Synopsys about the call-home data itself and how it was collected.

Synopsys finally produced the call-home data on Friday, December 1, and it raises more doubts about the relevance and proportionality of Synopsys' inspection requests. Notably, Synopsys' own data makes it clear that of the approximately 39,000 "acts of circumvention" allegedly identified by this call-home data, only *626* of them are identified to have occurred in the U.S.,

[2] The parties have reached an agreement regarding Defendant Tsai's devices, which are not subject to this motion.

[3] For example, Synopsys has requested to inspect *all* electronic devices used by certain individuals and user names that it claims are linked to uses of Synopsys' software based on its data. Defendants' counsel has explained repeatedly that many of the individuals whose devices would be covered by the requests lack the knowledge of *how to even use* Synopsys' software and thus could *not* have used the software (let alone in the U.S.), making inspection or imaging of their devices unnecessary. Furthermore, Synopsys claims that its requests include all MAC addresses included in its data, and suggests that Defendants could easily locate devices with those MAC addresses. Defendants, however, have not been able to locate devices with several of the MAC addresses. In addition, the requests include usernames that do not exist. Because the data was finally produced only recently, Ubiquiti has not been able to analyze it fully, or determine why it would have non-existent usernames or these other issues.

while the rest are identified to have occurred in Taiwan. Defendants request that the Court defer Synopsys' motion to compel, which seeks inspection of numerous computers and servers located in Taiwan, to allow the parties to brief a summary judgment motion on a narrow issue that is directly relevant to the requests: whether the DMCA has extraterritorial application to acts of circumvention that occurred on devices located outside of the U.S. An early summary judgment on this issue will guide the parties on the proper scope of Synopsys' forensic inspections, in view of their significant burden on Defendants, as discussed below, and would obviate the need for the Court to consider requests for devices that are not subject to Synopsys' DMCA claims.

Rule 34 "is not meant to create a routine right of direct access to a party's electronic information system," yet that is precisely what Synopsys seeks here, without any attempt to articulate a basis for good cause under Rule 26(b)(2)(B). *See* Fed. R. Civ. P. 34 Advisory Committee's Note.

Synopsys' requests to natively inspect and image non-server devices: Defendants have offered to make available forensic images of two computers used by Defendant Ching-Han Tsai for inspection at his counsel's U.S. office. Synopsys has agreed because, in addition to attorney-client and work-product privileged documents, these computers contain design source code files that fall under the "Highly Confidential – Layout Designs" designation in the protective order.

As for inspections or imaging of non-server devices used by other employees in Taiwan, it is not necessary for devices irrelevant to Synopsys' claims. Synopsys' call-home data identifies "USA" as the country where 626 alleged acts of circumvention occurred; "TWN," i.e., Taiwan, is identified as the country for *all* of the remaining entries in the call-home data. Because only acts of circumvention that occur *wholly* in the U.S. give rise to liability under the DMCA, Defendants need not turn over devices located in Taiwan. *See M Seven Sys. Ltd. v. Leap Wireless Int'l, Inc.*, 2014 WL 12026065, at *6 (S.D. Cal. June 4, 2014) ("If the modification occurred in South Korea or in another foreign nation, then the DMCA would have no application, because 'United States' copyright laws have no application to extraterritorial infringement.").

While Synopsys argues that forensic inspections of devices located both in and outside of the U.S. are nonetheless relevant to Synopsys' "domestic" DMCA claims, Synopsys has not explained what this means. Synopsys also has not articulated a basis for why a forensic inspection of a particular device—as opposed to an ordinary document production—is necessary for its trafficking, fraud, and RICO claims that are not based on how the software was used.[4] *See Memry Corp. v. Kentucky Oil Tech., N.V.*, 2007 WL 832937, at *3 (N.D. Cal. Mar. 19, 2007) ("a mere desire to check that the opposition has been forthright in its discovery responses is not a good enough reason" to warrant imaging; forensic inspection to obtain mirror image of drive is "extreme situation," including where computers have "a special connection to the lawsuit"); *Lee v. Stonebridge Life Ins. Co.*, 2013 WL 3889209, at *2 (N.D. Cal. July 30, 2013) (denying motion to compel forensic inspection of devices absent a showing that the information sought is not reasonably accessible through other sources).

[4] Significantly, Ubiquiti is not aware of anyone other than Defendant Tsai who may have used the software from the U.S., but it has not finished its analysis of the just produced call-home data.

Indeed, Synopsys' motion to compel inspection of the Taiwanese employees' devices at this point in time, without any clear justification, is premature and burdensome when Defendants are already collecting and producing responsive documents from Taiwanese employees who have relevant information, including any emails or license key files that would be the subject of Synopsys' "trafficking" claims. *See Irwin v. Mascott*, 2000 WL 35890723, at *6 (N.D. Cal. Aug. 28, 2000) (granting motion to compel imaging of drive only after thousands of relevant documents were unaccounted for); *Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc.*, 2012 WL 70428, at *1-2 (N.D. Cal. Jan. 9, 2012) (granting motion to compel inspection of drives only after witness admitted relevant files resided on drives and plaintiff unsuccessfully sought relevant documents); *Ameriwood Indus., Inc. v. Liberman*, 2006 WL 3825291, at *3 (E.D. Mo. Dec. 27, 2006) (granting motion to compel imaging only after plaintiff showed defendants failed to produce relevant emails).

Synopsys' requests to natively inspect or image server devices in Taiwan: Synopsys seeks a burdensome inspection or imaging of servers that are used daily in Defendants' largest R&D office for development and testing operations, and contain a vast amount of proprietary, confidential data that have no relevance whatsoever. R&D work would need to be halted during inspection or imaging. Further, imaging experts confirm that the 17-terabyte server/storage device arrangement in Taiwan is so complicated that they cannot guarantee that no work will be lost during imaging.

Defendants have collected some system logs from the servers and are working with forensic experts to determine if additional logs are available for collection. Synopsys has not explained why a native inspection is necessary before it receives Defendants' document production.[5] Nor has it explained the nature or length of the planned inspection, or even the software functionality that it believes constitutes an "act" of circumvention, all of which Defendants and the Court must understand to be able to assess the reasonableness of Synopsys' requests, the justification for imposing this burden and cost on Defendants, and, if possible, alternative options that would minimize the disruption to Defendants' business.

[5] Defendants have expressed this point since the parties started drafting this joint statement on November 22. Now, to finally address this point, Synopsys claims in this final statement that it needs a native inspection to obtain "evidence of network topography, configuration files, and virtual machine artifacts" and "forensic artifacts relevant to (i) use of key generators, (ii) use of piracy websites; (iii) external device usage; and (iv) user profiles." Synopsys raised these new inspection "needs" on December 8 but has not explained to Defendants' satisfaction *why* the information Synopsys seeks (such as network topography and the configuration files themselves, or the existence of any virtual machines or key generators) cannot be discovered through less burdensome means than a server inspection. Accordingly, Defendants are not in a position to address the newly stated purpose of Synopsys' inspection requests, other than to state that information Synopsys purports to seek from a native inspection of Defendants' systems may be obtained through less burdensome means. *See* Fed R. Civ. P. 34 Advisory Committee's Note ("Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.').

Sincerely,

/S/ Denise M. Mingrone
Denise M. Mingrone

Sincerely,

Jennifer Lee Taylor

CERTIFICATION OF MEET AND CONFER EFFORTS

I, Denise Mingrone, am an attorney representing Synopsys, Inc. in this matter. I hereby certify that I twice met, in person, with Defendants' counsel in an attempt to resolve this dispute. The first meeting occurred on November 3, 2017, and the second meeting occurred on November 8, 2017.

December 15, 2017 ________*/s/ Denise M. Mingrone*______

Denise Mingrone